

Title (en)
METHOD AND DEVICE FOR EXECUTING AN AUTHENTICATION SCHEME

Title (de)
VERFAHREN UND VORRICHTUNG ZUR AUSFÜHRUNG EINES AUTHENTIFIZIERUNGSSCHEMAS

Title (fr)
PROCÉDÉ ET DISPOSITIF D'EXÉCUTION D'UN SCHÉMA D'AUTHENTIFICATION

Publication
EP 3588841 A1 20200101 (EN)

Application
EP 18179235 A 20180622

Priority
EP 18179235 A 20180622

Abstract (en)
A method for executing an authentication scheme with a sender entity (10) and a receiver entity (20) is proposed, the method comprising: authenticating (201) a message (M) having a plurality of message parts (m₀-m₁₀) using a tree (T) of first hash functions (h₁-h₁₀) representing a hash function family of second hash functions, including: inputting (202) the message parts (m₀-m₁₀) into the tree (T) and calculating the first hash functions (h₁-h₁₀) for providing a hash value as an output (0₁₀) of said tree (T), wherein, in at least one of the first hash functions (h₁-h₁₀), one of the message parts (m₀-m₁₀) and an output (0₁-0₉) of one of the other first hash functions (h₁-h₉) are input.

IPC 8 full level
H04L 9/32 (2006.01)

CPC (source: EP)
H04L 9/3236 (2013.01)

Citation (applicant)

- J. LAWRENCE CARTER; MARK N. WEGMAN: "Universal Classes of Hash Functions", JOURNAL OF COMPUTER AND SYSTEM SCIENCES, vol. 18, no. 2, April 1979 (1979-04-01), pages 143 - 154
- MARK N. WEGMAN; J. LAWRENCE CARTER: "New Hash Functions and Their Use in Authentication and Set Equality", JOURNAL OF COMPUTER AND SYSTEM SCIENCES, vol. 22, 1981, pages 265 - 279, XP008003418, DOI: doi:10.1016/0022-0000(81)90033-7
- AYSAJAN ABIDIN; JAN-AKE LARSSON: "Direct Proof of Security of Wegman-Carter Authentication with Partially Known Key", QUANTUM INFORMATION PROCESSING, vol. 13, 2013, pages 2155 - 2170, XP035386335, DOI: doi:10.1007/s11128-013-0641-6
- BRECHT WYSEUR: "PhD Thesis", March 2009, KATHOLIEKE UNIVERSITEIT LEUVEN, article "White-Box Cryptography"

Citation (search report)

- [XYI] US 2017078101 A1 20170316 - MAXIMOV ALEXANDER [SE], et al
- [XYI] EP 2107711 A1 20091007 - FUJITSU LTD [JP]
- [XYI] US 2014245020 A1 20140828 - BULDAS AHTO [EE], et al
- [YD] WEGMAN M N ET AL: "NEW HASH FUNCTIONS AND THEIR USE IN AUTHENTICATION AND SET EQUALITY", JOURNAL OF COMPUTER AND SYSTEM SCIEN, ACADEMIC PRESS, INC., LONDON, GB, vol. 3, no. 22, 1 June 1981 (1981-06-01), pages 265 - 279, XP008003418, ISSN: 0022-0000, DOI: 10.1016/0022-0000(81)90033-7
- [YD] CARTER J L ET AL: "UNIVERSAL CLASSES OF HASH FUNCTIONS", JOURNAL OF COMPUTER AND SYSTEM SCIENCES, ACADEMIC PRESS, INC., LONDON, GB, vol. 18, 1 January 1979 (1979-01-01), pages 143 - 154, XP000652858, ISSN: 0022-0000, DOI: 10.1016/0022-0000(79)90044-8

Cited by
CN113676314A; EP3588843A1

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
EP 3588841 A1 20200101

DOCDB simple family (application)
EP 18179235 A 20180622